IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In Re Application Of:	§	**Atty. Docket No. RPS920030206US2**
	§	
RYAN CHARLES CATHERMAN	§	**Examiner: TURCHEN, JAMES R.**
	§	
Serial No.: 10/749,261	§	**Art Unit: 2139**
	§	
Filed: DECEMBER 31, 2003	§	**Conf. no.: 8466**
	§	
For: METHOD FOR SECURELY CREATING AN ENDORSEMENT CERTIFICATE UTILIZING SIGNING KEY PAIRS	§	

APPEAL BRIEF UNDER 37 C.F.R. 41.37

Mail Stop Appeal Briefs - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Sir:

This Brief is submitted in support of the Appeal of the Examiner's final rejection of Claims 1-6, 8, 10-22 and 24 in the above-identified application. A Notice of Appeal was filed in this case and received in the Patent Office on January 16, 2008. A two month extension of time is required and is hereby requested. Please charge the fee of $480.00 for the extension of time to **DILLON & YUDELL LLP Deposit Account No. 50-3083**. Please charge the fee of $510.00 due under 37 C.F.R. §1.17(c) for filing the brief, as well as any additional required fees, to **IBM's Deposit Account No. 09-0447**.

REAL PARTY IN INTEREST

The real party in interest in the present Application is International Business Machines Corporation, the Assignee of the present application as evidenced by the Assignment set forth at reel 014801, frame 0608.

RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences known to Appellants, the Appellants' legal representative, or assignee, which directly affect or would be directly affected by or have a bearing on the Board's decision in the pending appeal.

STATUS OF CLAIMS

Claims 1-6, 8, 10-22 and 24 stand finally rejected by the Examiner as noted in the Final Office Action dated August 16, 2007. The rejection of Claims 1-6, 8, 10-22 and 24 is appealed.

STATUS OF AMENDMENTS

Appellants' Amendment A, filed on June 8, 2007, was entered by the Examiner, as noted in the Final Office Action. No amendment was made subsequent to the Final Action from which this appeal is taken.

SUMMARY OF THE CLAIMED SUBJECT MATTER

As recited by Appellants' example method Claim 1 (and similarly configured system Claim 17), Appellants' invention provides a method (FIGs. 4 and 5) for securely creating an endorsement certificate for a device in an insecure environment. The method comprises: generating for a valid device (FIG. 2) an endorsement key pair that includes a private key and a public key, wherein said private key is not public readable (¶¶ 0036, 0039; FIG. 4, 403); creating a non-public, signing key pair that is injected into a plurality of valid devices, wherein the signing key pair is a first signing key pair that is provided to a first set of said plurality of valid devices and a second set of said plurality of valid devices are provided a second signing key pair, based on a pre-defined method for determining when to switch from utilizing said first signing key pair to utilizing said second signing key pair, said pre-defined method selected from among: expiration of a preset amount of device manufacturing time; and manufacture of a preset number

of devices from the plurality of valid devices (*see* ¶ 0040, 0041). The method further comprises: verifying at a credential server that an endorsement key of a requesting device is a valid endorsement key generated during manufacture of said valid device by confirming a signature of said endorsement key is a public signing key of said signing key pair, wherein said credential server includes secure identification data of said non-public, signing key pair (*see* ¶ 0045, 0046; FIG. 4, 415, 416); and inserting an endorsement certificate into said device to indicate that said device is an approved device by an OEM (original equipment manufacturer) of the device only when said endorsement key is confirmed having been generated from within a valid device (*see* ¶ 0046, 0047; FIG. 4, 417, 419, 421; *see* also FIG. 5, ¶¶ 0049-0051). The signing key pair is a single-use parameter (¶ 0044), and the method further comprises immediately destroying said signing key pair within said device following a creation of said endorsement key (EK) (¶ 0044).

Appellants' Claim 13 (incorporating the features of base Claim 12) further provides a data processing system comprising: a processor 150; a trusted platform module (TPM) chip 150; a bus for interconnecting said processor and said TPM chip; a network interface with communication means for connecting said TPM to a secure credential server 107; and means, whereby said TPM 150 is able to verify an endorsement key (EK) pair of said TPM as being a valid pair generated during manufacture of said TPM by utilizing a signing key pair injected by a TPM vendor into the TPM during manufacture (103) of the TPM, wherein said signing key pair is a single-use parameter (¶ 0044), said data processing system further comprising means for immediately destroying said parameter within said device following a creation of the EK (¶ 0044). The signing key pair has an associated signing key certificate that is sent to the secure credential server during manufacture of the TPM (¶ 0045). The means for verifying an endorsement key pair further comprises: means for signing a public value of said endorsement key pair with a public signing key of said signing key pair to generate a signed (EK) (¶¶ 0045-0046); and means for forwarding said signed EK to said credential server, wherein said credential server returns an endorsement certificate only when the signed EK was generated within the TPM as confirmed by a comparison of the signed EK's public signing key with a public signing key of the signing key certificate (¶¶ 0045-0047; FIG. 4; *see* also FIG. 5, ¶¶ 0049-0051).

Similarly, Claim 14 provides a data processing system 104 utilized for issuing endorsement certificates. The data processing system 104 comprises: a processor; a memory couple to said processor via an interconnect; a security mechanism for ensuring optimum security of processes within said data processing system; input/output mechanism for receiving a signing key certificate from a TPM vendor for utilization during a credential process for a specific group of manufactured TPM devices; and secure communication means for receiving an endorsement key (EK) requesting issuance of an endorsement certificate, wherein said EK comprises a public endorsement key signed by a public signing key. Further, the data processing system comprises program means for: determining, by utilizing said public signing key and said signing key certificate, when said EK is an EK of an endorsement key pair that was generated within one of said manufactured TPM devices; recording when a request for EK certificate fails (FIG. 4, 423; ¶ 48; *see* also FIG. 5, ¶¶ 0049-0051); tracking each failed request to identify TPM vendors with greater than a pre-established number of failures; and messaging said TPM vendors to update their security procedures (*id.*).

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A. The Examiner's rejection of Claims 1-6, 8, 10-22 and 24 under 35 U.S.C. §103(a) as being unpatentable over *Challener* (U.S. Patent Publication No. 2002/0169717) in view of *Smith* (U.S. Patent No. 6,233,685) and further in view of *Wood* (U.S. Patent Publication No. 2006/0072747) is to be reviewed on Appeal.

B. The Examiner's rejection of Claims 14-16 under 35 U.S.C. §103(a) as being unpatentable over *Challener* in view of *Drake* (U.S. Patent No. 6,347,374) is to be reviewed on Appeal.

ARGUMENT

A. The rejection of Claims 1-6, 8, 10-22 and 24 as being unpatentable over *Challener* in view of *Smith* and further in view of *Wood* is not well founded and should be reversed.

A. 1 General requirements for a claim rejection under 35 U.S.C. § 103

According to 35 U.S.C. §103(a):

> A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject

matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

In order to make the obviousness determination, the U.S. Supreme Court held in Graham v. John Deere Co., 383 U.S. 1 (1966) (hereinafter *John Deere*) that three factors must be considered:

(1) the scope and content of the pertinent prior art;
(2) differences between the pertinent prior art and the invention at issue; and
(3) the ordinary level of skill in the pertinent art.

In KSR Intern. Co. v. Teleflex, Inc., 127 S.Ct. 1727 (2007), the U.S. Supreme Court clarified that a non-obviousness determination must include an inquiry as to "whether the improvement is more than the predictable use of prior art elements according to their established functions."

A.2 The combination of *Challener*, *Smith* and *Wood* does suggest to one of skilled in the art the subject matter of Appellants' Example Claim 1.

The combination of *Challener*, *Smith* and *Wood* does not render Appellants' claimed invention unpatentable because the combination does not suggest the subject matter recited by Appellants' independent claims, given the first and second prongs of *John Deere*. Specifically, one skilled in the art would not find several features recited by Appellants' independent claims to be suggested by the references or the various combinations thereof. Among the features that are not suggested by the references or the combinations thereof are the following:

> (1) ...wherein the signing key pair is a first signing key pair that is provided to a first set of said plurality of valid devices and a second set of said plurality of valid devices are provided a second signing key pair, based on a pre-defined method for determining when to switch from utilizing said first signing key pair to utilizing said second signing key pair, said pre-defined method selected from among:
>
> expiration of a preset amount of device manufacturing time; and
>
> manufacture of a preset number of devices from the plurality of valid devices;
>
> (2a) verifying at a credential server that an endorsement key of a requesting device is a valid endorsement key generated during manufacture of said valid device ...; and
>
> (2b) inserting an endorsement certificate ... only when said endorsement

key is confirmed having been generated from within a valid device; and

(3) wherein said signing key pair is a single-use parameter, ... immediately destroying said signing key pair ... following a creation of said EK.

The specific sections of *Challener*, *Smith*, and *Wood* being relied upon to support the rejections of the above elements are devoid of any teaching of those elements. In providing the rejections, Examiner appears to mischaracterize the references and/or misinterpret the teachings of Appellants' claims. Examiner then relies on these mischaracterizations and/or several conclusory statements to support the rejection of the specific features of Appellants' claims. For example, ¶ 0024 of *Challener* does not teach or suggest the specific criteria for performing the inserting of the endorsement certificate into the device, namely "only when said endorsement key is confirmed..." Examiner does not address this clear deficiency in *Smith* and appears to have overlooked this requirement of the claim element.

As another example, with respect to changing of the signing key based on a predefined method (which methods are specifically defined), Examiner rejects that feature of Appellants' claims without providing any support from within the references. Rather, Examiner relies on a conclusory statement that such a feature would be obvious. Absent some reference on which to base this rejection, Appellants believe the rejection to be unfounded and reversible. The changing of a key from device to device is not synonymous with or suggestive of the specific implementation steps provided by Appellants' claim features.

With respect to the single use character of the signing key pair, Examiner relies on *Wood* to support the rejection of this feature. First, Appellants believe that the combination of *Wood* with *Challener* and *Smith* is improper as there is no motivation within the references, outside of a desire to follow the teachings taken from Appellants' claimed invention, to combine *Woods* with these other references. *Wood* is directed to an non-analogous art.

However, assuming there is support for the combination, a careful reading of *Woods* reveals that *Wood* does not teach or suggest the feature being rejected based on *Wood*. For example, ¶ 0039 of *Wood* fails to teach or suggest a single-use signing key pair that is destroyed

following creation of the EK. In fact that section merely describes adding "random states from one or more external sources ... when gathering seeding information," and "eliminating cryptographic breaks into a system by having strong and remote sources of randomness." Clearly, this paragraph is devoid of any suggestion of the features that the paragraph was cited to reject. Thus, none of the references provide support for the rejection of this feature of Appellants' example claim.

For the above reasons, one skilled in the art would not find Appellants' invention unpatentable over the combination of references. The above claims are therefore allowable over the combination, and Examiner's rejection of these claims is not well founded and should be reversed.

B. The rejection of Claims 14-16 under 35 U.S.C. §103(a) as being unpatentable over *Challener* in view of *Drake* is not well founded and should be reversed.

First, Appellants assert that the above combination are improper. Second, even if found to be proper, the combination would still not render Appellants' claimed invention unpatentable because the combination does not suggest the subject matter recited by Appellants' claims to one skilled in the art at the time of Appellants' invention.

B.1. No motivation to combine

First, with respect to the above references, there is no motivation to combine *Drake* with *Challener* in the manner done by the Examiner. The proper rationales for arriving at a conclusion of obviousness, as indicated by the U.S. Supreme Court in the case of *KSR International Co. v. Teleflex, Inc. et al.*, 127 S. Ct. 1727 (2007), hereinafter *KSR*, include the following tests for determining a motivation to combine elements from the prior art:

A. Combining prior art elements according to known elements to yield predictable results;
B. Simple substitution of one known element for another to obtain predictable results;
C. Use of a known technique to improve similar devices in the same way;
D. Applying a known technique to a known device ready for improvement to yield predictable results;

E. "Obvious to try" – choosing from a finite number of identified, predictable solutions, with a reasonable expectation of success;

F. Some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the prior art reference or to combine prior art reference teachings to arrived at the claimed invention.

(all emphasis added.)

There is no teaching within *Drake* or *Challener* that would motivate one skilled in the art at the time of Appellants' invention to combine the features of the two references. Further, there is no motivation or support for the proposed combination of *Drake* and *Challener* in either reference or under any of the above *KSR* rationales for making a proper combination under §103. Therefore, the combination is improper.

On page 9 of the Office Action, in explaining the motivation to combine *Kolawa* and *Looney*, Examiner states: "[i]t would have been obvious to one of ordinary skill in the art ... to modify teaching the system ... with the event auditing system ... in order to detect intrusion and misuse of data processing systems." It is therefore clear that, under *KSR*, Examiner relies on the "teaching, suggestion, and motivation" test with the rationale of "obvious to one of ordinary skill in the art" to support the combination and determine obviousness.

Appellants' respectfully disagree with Examiner's conclusions under this rationale because the two references practice in different arts, and do not themselves suggest, teach or motivate one skilled in the art to make the combination. Any possible connection between the teachings of *Looney* with the teachings of *Kolawa* would be so tangential in nature that one skilled in the relevant art would not have been inclined to combine the two references. There is, therefore, no support within the references themselves for combining the references, and one skilled in the art would not have been motivated to combine the references. Thus, Appellants again assert that this combination is improper.

B.2 Hindsight reasoning for combining references not allowed under §103

Since, as explained above, the references themselves do not teach or suggest their combination, it thus appears that Examiner has relied on a teaching of Appellants' claimed invention to find motivation for the above combination. In rejecting claims under 35 U.S.C.

§103, Examiner is expected to make the factual determinations set forth in Graham v. John Deere Co., 383 U.S. i, 17, 148 USPQ 459, 467 (1966). Examiner is also expected to provide a reason why one having ordinary skill in the pertinent art would have been led to modify the prior art or to combine prior art references to arrive at the claimed invention. Such reason must stem from some teaching, suggestion or implication in the prior art as a whole or knowledge generally available to one having ordinary skill in the art, following at least one of the above rationales listed by *KSR*. Given the failure of either reference to teach or suggest the combination and the lack of a proper *KSR* rationale for the combination, it appears that Examiner has relied on the teachings of Appellants' claimed invention in deciding on the combination.

However, it is further clearly established that "[d]etermination of obviousness cannot be based on the hindsight combination of components selectively culled from the prior art to fit the parameters of the patented invention." *ADT Corp. v. Lydall, Inc.*, 289 F.3d 1367, 62 USPQ2d 1917 (Fed. Cir. 2002). Examiner cannot therefore rely on Appellants' claimed invention to support the §103 rejection. Since the references fail to support the combination, the combination is not valid, and Appellants' claims are allowable over the references.

B.3. The combinations fail to teach or suggest the claimed invention

Even if support could be found for the combinations, those combinations would still not render Appellants' claimed invention obvious to one of skill in the art because the combinations fail to teach or suggest several features recited by Appellants' claims, including those features described above in the arguments overcoming the rejection of example Claim 1. Additionally, *Drake* does not teach or suggest the specific features related to recording when an EK certificate fails and tracking the failed request and messaging the TPM vendors.

The above deficiencies in the teachings/suggestions of *Challener* and *Drake* indicate that the combination of these references does not teach or suggest several features recited within Appellants' claims. Thus, One skilled in the art would not find Appellants' invention unpatentable over the combination of references. Appellants' Claim 14-16 are therefore allowable over the combination, and Examiner's rejection of these claims is not well founded and should be reversed.

CONCLUSION

Appellants have pointed out with specificity the manifest error in the Examiner's rejections and the claim language which renders the invention patentable over the primary reference and the various combinations of references. Appellants, therefore, respectfully request that this case be remanded to the Examiner with instructions to issue a Notice of Allowance for all pending claims.

Respectfully submitted,

/Eustace P. Isidore/

Eustace P. Isidore
Reg. No. 56,104
DILLON & YUDELL LLP
8911 N. Capital of Texas Highway
Suite 2110
Austin, Texas 78759
512-343-6116

ATTORNEY FOR APPELLANTS

APPENDIX

1. A method for securely creating an endorsement certificate for a device in an insecure environment, said method comprising:

generating for a valid device an endorsement key pair that includes a private key and a public key, wherein said private key is not public readable;

creating a non-public, signing key pair that is injected into a plurality of valid devices, wherein the signing key pair is a first signing key pair that is provided to a first set of said plurality of valid devices and a second set of said plurality of valid devices are provided a second signing key pair, based on a pre-defined method for determining when to switch from utilizing said first signing key pair to utilizing said second signing key pair, said pre-defined method selected from among:

expiration of a preset amount of device manufacturing time; and

manufacture of a preset number of devices from the plurality of valid devices;

verifying at a credential server that an endorsement key of a requesting device is a valid endorsement key generated during manufacture of said valid device by confirming a signature of said endorsement key is a public signing key of said signing key pair, wherein said credential server includes secure identification data of said non-public, signing key pair; and

inserting an endorsement certificate into said device to indicate that said device is an approved device by an OEM (original equipment manufacturer) of the device only when said endorsement key is confirmed having been generated from within a valid device;

wherein said signing key pair is a single-use parameter, said method further comprising immediately destroying said signing key pair within said device following a creation of said endorsement key (EK).

2. The method of Claim 1, further comprising:

providing a signing key certificate for said signing key pair, said signing key certificate including a public signing key of said signing key pair; and

forwarding said signing key certificate via a secure communication medium to said credential server.

3. The method of Claim 1, further comprising:

signing said public key of the endorsement key pair with a public signing key of said signing key pair when creating the endorsement key (EK); and

forwarding a resulting signed EK to said credential server to initiate a credential process.

4. The method of Claim 3, further comprising:

receiving said signed EK at said credential server;

comparing the public signing key within the signing key certificate with a signature from the signed EK; and

when the public signing key matches the signature, confirming said EK as originating from a valid device.

5. The method of Claim 1, wherein following said verifying step said method further comprises:

initially storing the credential in a database of said credential server;

monitoring for a request from a customer to provide said certificate to said device; and

following a receipt of said customer request, transmitting said certificate to said device to be inserted within the device.

6. The method of Claim 1, wherein said endorsement certificate is once-writeable public-readable and is utilized for signing said public key during communication from and to said device.

7. (canceled)

8. The method of Claim 1, wherein said credential server is remotely located from a vendor manufacturing said device and said method comprises transmitting said signing key pair from said device to said credential server via a secure communication medium.

9. (canceled)

10. The method of Claim 1, wherein said device is a trusted platform module (TPM).

11. A TPM device manufactured and authenticated according to the steps of Claim 1.

12. A data processing system comprising:

a processor;

a trusted platform module (TPM) chip;

a bus for interconnecting said processor and said TPM chip;

a network interface with communication means for connecting said TPM to a secure credential server; and

means, whereby said TPM is able to verify an endorsement key (EK) pair of said TPM as being a valid pair generated during manufacture of said TPM by utilizing a signing key pair injected by a TPM vendor into the TPM during manufacture of the TPM, wherein said signing key pair is a single-use parameter, said data processing system further comprising means for immediately destroying said parameter within said device following a creation of the EK.

13. The data processing system of Claim 12, wherein said signing key pair has an associated signing key certificate that is sent to the secure credential server during manufacture of the TPM and said means for verifying an endorsement key pair further comprises:

means for signing a public value of said endorsement key pair with a public signing key of said signing key pair to generate a signed (EK); and

means for forwarding said signed EK to said credential server, wherein said credential server returns an endorsement certificate only when the signed EK was generated within the TPM as confirmed by a comparison of the signed EK's public signing key with a public signing key of the signing key certificate.

14. A data processing system utilized for issuing endorsement certificates, comprising:

a processor;

a memory couple to said processor via an interconnect;

a security mechanism for ensuring optimum security of processes within said data processing system;

input/output mechanism for receiving a signing key certificate from a TPM vendor for utilization during a credential process for a specific group of manufactured TPM devices; and

secure communication means for receiving an endorsement key (EK) requesting issuance of an endorsement certificate, wherein said EK comprises a public endorsement key signed by a public signing key; and

program means for:

determining, by utilizing said public signing key and said signing key certificate, when said EK is an EK of an endorsement key pair that was generated within one of said manufactured TPM devices;

recording when a request for EK certificate fails;

tracking each failed request to identify TPM vendors with greater than a pre-established number of failures; and

messaging said TPM vendors to update their security procedures.

15. The data processing system of Claim 14, further comprising means for generating a certificate only when said public signing key matches a public signing key within said signing key certificate.

16. (canceled)

17. A system for securely creating an endorsement certificate for a device in an insecure environment, said system comprising:

means for generating for a valid device an endorsement key pair that includes a private key and a public key, wherein said private key is not public readable;

means for creating a non-public, secure value that is provided to both a plurality of valid devices and a credential server, wherein the signing key pair is a first signing key pair that is provided to a first set of said plurality of valid devices and a second set of said plurality of valid devices are provided a second signing key pair, based on a pre-defined system for determining when to switch from utilizing said first signing key pair to utilizing said second signing key pair, said pre-defined system selected from among:

expiration of a preset amount of device manufacturing time; and

manufacture of a preset number of devices from the plurality of valid devices;

means for verifying at a credential server that an endorsement key (EK) of a requesting device is a valid endorsement key generated during manufacture of said valid device by confirming a signature of said endorsement key is a public signing key of said signing key pair, wherein said credential server includes secure identification data of said non-public, signing key pair; and

means for inserting an endorsement certificate into said device to indicate that said device is an approved device by an OEM (original equipment manufacturer) of the device only when said endorsement key is confirmed having been generated from within a valid device;

wherein said signing key pair is a single-use parameter, said system further comprising means for immediately destroying said parameter within said device following a creation of said EK.

18. The system of Claim 17, further comprising:

means for providing a signing key certificate for said signing key pair, said signing key certificate including a public signing key of said signing key pair; and

means for forwarding said signing key certificate via a secure communication medium to said credential server.

19. The system of Claim 18, further comprising:

means for combining said public key of the endorsement key pair with a public signing key of said signing key pair when creating the endorsement key (EK); and

means for forwarding a resulting signed EK to said credential server to initiate a credential process.

20. The system of Claim 19, further comprising:

means for receiving said EK from said credential server;

means for comparing the copy of the public signing key within the signing key certificate with a signature from the signed EK; and

means, when the public signing keys match, for confirming said EK as originating from a valid device.

21. The system of Claim 17, wherein following said verifying said system further comprises:

means for initially storing the credential in a database of said credential server;

means for monitoring for a request from a customer to provide said certificate to said device; and

means for following a receipt of said customer request, transmitting said certificate to said device to be inserted within the device.

22. The system of Claim 17, wherein said endorsement certificate is once-writeable public-readable and is utilized for signing said public key during communication from and to said device.

23. (canceled)

24. The system of Claim 17, wherein said credential server is remotely located from a vendor manufacturing said device and said system comprises means for transmitting said signing key certificate from said device to said credential server via a secure communication medium.

25. (canceled)

EVIDENCE APPENDIX

Other than the Office Action(s) and reply(ies) already of record, no additional evidence has been entered by Appellants or the Examiner in the above-identified application which is relevant to this appeal.

RELATED PROCEEDINGS APPENDIX

There are no related proceedings as described by 37 C.F.R. §41.37(c)(1)(x) known to Appellants, Appellants' legal representative, or assignee.